WWW Technology in the Formal Evaluation of Trusted Systems

E.J. McCauley
Trusted Systems Project Manager
Silicon Graphics Computer Systems Inc.
2011 N. Shoreline Blvd.
Mt. View, California

Abstract

The World Wide Web (WWW) introduces exciting possibilities for the use of new technology in the formal evaluation of trusted systems. This is a report of a work in progress. It discusses the conceptual foundations of the WWW use in formal evaluations of a the security properties of a system, and offers some of the initial insights gained in its use. Silicon Graphics® is using this structure for the submittal of documentation for the formal evaluation of the Trusted IRIX™/CMW 6.2 operating system.

Background

The World Wide Web is... This is an extremely difficult sentence to complete. On the purely objective level it is an extremely loose federation of independent systems connected to the Internet that offer support for the simple protocols used to retrieve information and display it. This explanation, while factually correct, trivializes the impact of this technology. The WWW empowers its users in a way that no previous technology has since the invention of the printing press. Essentially every user can create connections between concepts that are unique to the individual.

Users access the web through client programs called “browsers." These programs are available for essentially all personal computers and workstations. The browser retrieves information from a server by making a request using a simple name called a Uniform (or Universal) Resource Locator, “URL." These are the cryptic strings starting to be found at the end of advertisements. URLs describe the location, file and accessing protocol for the information. For example, `http://www.sgi.com/index.html` says how to access the information, here use the HyperText Transport Protocol, “http”; which system is to be accessed, here “sgi.com”; and the specific file or “web page”, here “index.html”, which also the default name if it was omitted. The information retrieved identifies its own format, so the appropriate processing by the browser may be performed to present it to the user, e.g., display text or images, play sounds or movies, or even navigate through a downloaded 3D virtual world.

One of the most powerful aspects of the WWW is the use of the Hypertext Markup Language (HTML). HTML allows the connection of documents through hypertext links. In essence, any point in one document can be connected to an arbitrary point in another document anywhere on the WWW.

In cooperation with the National Security Agency, Silicon Graphics Computer Systems Inc. (SGI) is using this technology in the submission of materials for the formal evaluation of Trusted IRIX/CMW 6.2. We feel that the use of WWW technology has the potential to significantly improve the timeliness and thoroughness of formal evaluations.

Genesis of the Concept

As the National Computer Security Center team completed the formal evaluation of the Trusted IRIX™/B 4.0.5 EPL operating system, the team at SGI universally felt “there must be a better way” to produce and submit the evaluation materials. Significant resources were expended to ensure consistency of points stated in several different documents. It was difficult to take “vertical slices” through the over 3,000 pages of submitted material to explore some specific topic from its highest level discussion down to the details of test results. The material had been developed using the “venerable” *troff* program, which required a great deal of effort to achieve the desired format.

SGI had switched to on-line electronic documentation in 1992, so there was considerable internal experience with production of documents for the IRIS Insight™ viewer. This package is based on the Standard Generalized Markup Language (SGML), and features a rich environment with embedded figures, audio, and full document indexing for rapid access by keyword searches. However, on further research, it became clear that the richness of the Insight environment came at a cost in the difficulty of creating the documents. While such efforts could be justified for customer deliverable documents, this approach appeared to be just trading one set of problems for another for evaluation submittal documents.

Fortunately, SGI had begun to embrace the WWW technology both as internal information management vehicle, and as a product technology. The first WWW products from SGI, the WebFORCE™ family of products, were released at nearly the same time as the completion of the formal evaluation of Trusted IRIX/B 4.0.5 EPL in the spring of 1994. The team began a low intensity "proof of concept" experiment of casting portions of the submittal materials into web pages. This initial experiment was extremely successful. In very short order, the team decided that our next evaluation would be documented using web pages.

As work began on the next generation system, Trusted IRIX/CMW 6.2, we elected to do all design documents as web pages. As they were completed and reviewed, they were woven into the expanding web of documentation for the system. It was also fairly easy to "recycle" the previous evaluation documents into HTML and to update them. This effort was aided by the WebMagic™ editor, a screen oriented editor for HTML. One of the helpful features of WebMagic is the ability to establish hypertext links within and between documents with a simple point and click interface. HTML documents could also be edited with conventional text editors, and could be managed through our standard configuration management tools.

A system evaluation is a cooperative effort between the vendor and the team assembled by NSA/NCSC. If the documentation were to be submitted as web pages, it would be necessary to seek NSA approval for this form of submittal. It is difficult to appreciate Web technology in the abstract, so the SGI team decided that the most effective way to present the concept would be to relate it to the guidelines for submittals produced by the Process Action Team Guidance Working Group, which had established guidelines for the submittal of information to NSA/NCSC for formal evaluation of systems. In August 1995, SGI presented a demonstration of the technology for NSA/NCSC. This demonstration showed an HTML version of the "PAT Working Group Form and Content of Vendor Design Documentation" report, which linked into the top level description of Trusted IRIX/B 4.0.5 EPL found in the Final Evaluation Report, which had also been converted to HTML. The sections of the Final Evaluation Report were linked into the major design documents for the system. Additional linkage structures tied in the system manual pages (primary interface documentation), test plans and test results. The overall structure is shown in Figure 1.

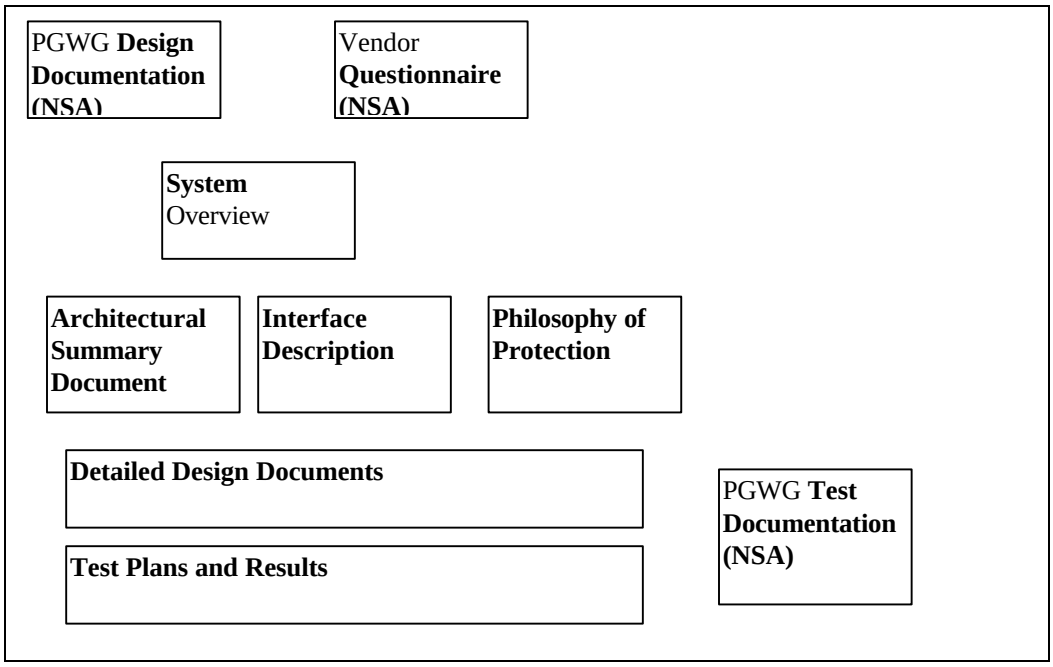

Figure 1 -Overall Web Structure

The demonstration generated considerable interest, and by the time of the 1995 National Information Security Conference, NSA had convened an informal working group, dubbed the “Hypertext Working Group," to provide more details and guidelines for the use of WWW technologies in the submittal of formal evaluation documentation. This team submitted its report to NSA in February 1996. At the outset, the report urged flexibility to make maximum use of emerging technology. The report suggested starting with the two PGWG reports, and the NCSC Vendor Questionnaire. This illustrates a strength of the WWW technology. These three documents point to the same underlying information in the submittal. Depending on the nature of the task at hand, the evaluation team can access the information through several different paths. This principle can be extended by creating other access paths structured to needs of the evaluation team. Most browsers also support more informal indexing through their ability to create “bookmarks," URLs that are used to “remember” interesting content and rapidly return to it.

Browsers also facilitate information access by remembering the path used to reach some URL, and being able to backtrack to earlier points in the search. This allows an evaluator to research a specific detail and to go back to where the search started to look at other information.

One area that received much attention and discussion by the Hypertext Working Group was the mechanisms for coordination and feedback between the evaluation team and the vendor. These efforts are collaborative, and there is a need to generate feedback to the vendor, for the vendor to respond by altering the system software and documentation, and for the team to be able to assess the results looking at “before and after” content. Several different mechanisms were discussed, and recommendations were made to provide links to “before” content in the “after” document. More sophisticated schemes involving on the fly generation of the differences were also considered. Support for annotation of documents is a very active development area for the Web, so new technologies may overtake these recommendations.

The use of WWW technology changes the environment as compared to conventional document submittals. The most significant of these changes is that HTML documents lack a page structure. This means that conventional schemes like indices and tables of contents must be replaced by hypertext links. The lack of a page structure also posed challenges for the appropriate marking of vendor confidential materials. Many evaluation submittals contain information that the vendor considers sensitive, which must be clearly

indicated to the members of the evaluation team. SGI is exploring several ways to do this; one approach has been to have a background that indicates the sensitivity of the document, as well as specific sensitivity markings at the beginning and end of the document.

An unexpected issue arose as the working group discussed the mechanics of the evaluation. Many evaluators work in environments with poor or non-existent connectivity to the external Internet, due to the security considerations of their environments. To address this, the working group recommended that the evaluation submittal be self contained and not contain links to sites on the Internet. This is somewhat unfortunate for the SGI submittal, as much of the material on the processors and systems is available as web pages on the SGI and MIPS® Technology Inc. corporate web pages. The submittal package has made copies of this material for use by the evaluation team.

Conclusions

Since the evaluation of Trusted IRIX/CMW 6.2 is not complete, it is a little premature to draw too many conclusions. Still, a number of things have emerged from the initial work. Most important is that the existing framework for evaluation submittals fits well to the new technology of the web. It has been straightforward to take documents developed for conventional submittals and adapt their structure to a web based submittal. We have found that creation and management of web based documents is actually easier than the techniques used in the earlier evaluation, especially since there is very active tool development to aid the task.

Acknowledgements

This work has been a collaboration of many peoples' efforts. In addition to the SGI Trusted IRIX™ team, we appreciate the support of Dennis Kinch, Janine Pedersen and Rita Montequin of NSA in seeing the potential of the work and establishing the Hypertext Working Group. The working group, Jim Reynolds (MITRE), Richard Waltzer (MITRE), Al Nims (Aerospace), Jack Walsh (NSA), and Casey Schaufler (SGI) all contributed insights and observations that materially improved the initial ideas.

Trademarks